09818391 46

(translation of the front page of the priority document of Japanese Patent Application No. 2000-091316)

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: March 29, 2000

Application Number : Patent Application 2000-091316

Applicant(s) : Canon Kabushiki Kaisha

April 20, 2001

Commissioner,
Patent Office Kouzo OIKAWA

Certification Number 2001-3033060

09/818,391

CFO 15244 US #4
HY/fu

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年 ４月２５日

出願番号
Application Number: 特願２０００－１２４８２７

出願人
Applicant(s): キヤノン株式会社

２００１年 ４月２０日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願
【整理番号】　4027068
【提出日】　平成12年 4月25日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 13/00
【発明の名称】　ネットワークシステム、リモートアクセス実行装置、方法、及びコンピュータ読み取り可能な記憶媒体
【請求項の数】　34
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　京徳　諭
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代理人】
【識別番号】　100090273
【弁理士】
【氏名又は名称】　國分　孝悦
【電話番号】　03-3590-8901
【手数料の表示】
【予納台帳番号】　035493
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9705348
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ネットワークシステム、リモートアクセス実行装置、方法、及びコンピュータ読み取り可能な記憶媒体

【特許請求の範囲】

【請求項１】　所定の装置間でのリモートアクセスを可能としたネットワークシステムであって、

上記所定の装置のうち一方の装置は、自機の位置情報を取得する位置情報取得手段と、上記位置情報取得手段により取得された上記位置情報を送信する送信手段を備え、

上記所定の装置のうち他方の装置は、上記送信手段により送信された上記位置情報を受信する受信手段と、上記受信手段により受信された上記位置情報が所定範囲内にあるか否かを照合する照合手段とを備えることを特徴とするネットワークシステム。

【請求項２】　所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、

自機の位置情報を取得する位置情報取得手段と、

上記所定の装置との間のリモートアクセス時に、上記位置情報取得手段により取得された上記位置情報を上記所定の装置に送信する送信手段とを備えたことを特徴とするリモートアクセス実行装置。

【請求項３】　上記位置情報取得手段は、ＧＰＳ受信機により上記位置情報を取得することを特徴とする請求項２に記載のリモートアクセス実行装置。

【請求項４】　所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の位置情報を受信する受信手段と、

上記受信手段により受信された上記位置情報が所定範囲内にあるか否かを照合する照合手段とを備えたことを特徴とするリモートアクセス実行装置。

【請求項５】　上記照合手段により上記位置情報が上記所定範囲内にないと判断された場合、リモートアクセスを切断するリモートアクセス切断手段を備え

たことを特徴とする請求項４に記載のリモートアクセス実行装置。

【請求項６】　上記照合手段は、上記所定の装置との間のリモートアクセス中に繰り返し照合を行うことを特徴とする請求項４又は５に記載のリモートアクセス実行装置。

【請求項７】　所定の装置間でのリモートアクセスを可能としたネットワークシステムであって、

上記所定の装置のうち一方の装置は、自機のＩＤ情報を取得するＩＤ情報取得手段と、上記ＩＤ取得手段により取得された上記ＩＤ情報を送信する送信手段を備え、

上記所定の装置のうち他方の装置は、上記送信手段により送信された上記ＩＤ情報を受信する受信手段と、上記受信手段により受信された上記ＩＤ情報によるＩＤが所定ＩＤであるか否かを照合する照合手段とを備えることを特徴とするネットワークシステム。

【請求項８】　所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、

自機のＩＤ情報を取得するＩＤ情報取得手段と、

上記所定の装置との間のリモートアクセス時に、上記ＩＤ情報取得手段により取得された上記ＩＤ情報を上記所定の装置に送信する送信手段とを備えたことを特徴とするリモートアクセス実行装置。

【請求項９】　上記ＩＤ情報取得手段は、自機の所定個所或いは自機に使用される部材の所定個所に書き込まれたＩＤを読み取って取得することを特徴とする請求項８に記載のリモートアクセス実行装置。

【請求項１０】　半導体製造装置であることを特徴とする請求項８に記載のリモートアクセス実行装置。

【請求項１１】　上記ＩＤはレチクル、レンズ、ウェハ、ステージ、レチクル基準マークのうち少なくともいずれか一に書き込まれていることを特徴とする請求項１０に記載のリモートアクセス実行装置。

【請求項１２】　上記ＩＤを光学的に読み取る光学系読み取り手段を備えたことを特徴とする請求項１１に記載のリモートアクセス実行装置。

【請求項１３】　所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置のＩＤ情報を受信する受信手段と、

上記受信手段により受信された上記ＩＤ情報によるＩＤが所定ＩＤであるか否かを照合する照合手段とを備えたことを特徴とするリモートアクセス実行装置。

【請求項１４】　上記照合手段により上記ＩＤ情報によるＩＤが上記所定ＩＤでないと判断された場合、リモートアクセスを切断するリモートアクセス切断手段を備えたことを特徴とする請求項１３に記載のリモートアクセス実行装置。

【請求項１５】　上記照合手段は、上記所定の装置との間のリモートアクセス中に繰り返し照合を行うことを特徴とする請求項１３又は１４に記載のリモートアクセス実行装置。

【請求項１６】　所定の装置間でのリモートアクセスを可能としたネットワークシステムであって、

上記所定の装置のうち一方の装置は、自機の第１の位置情報を取得する位置情報取得手段と、自機の第２の位置情報が予め組み合わされているＩＤ情報を取得するＩＤ情報取得手段と、上記第１の位置情報及び上記ＩＤ情報を送信する送信手段を備え、

上記所定の装置のうち他方の装置は、上記送信手段により送信された上記第１の位置情報及び上記ＩＤ情報を受信する受信手段と、上記第１の位置情報と上記ＩＤ情報に組み合わされている上記第２の位置情報とを照合する照合手段とを備えることを特徴とするネットワークシステム。

【請求項１７】　所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、

自機の第１の位置情報を取得する位置情報取得手段と、

自機の第２の位置情報が予め組み合わされているＩＤ情報を取得するＩＤ情報取得手段と、

上記所定の装置との間のリモートアクセス時に、上記第１の位置情報及び上記ＩＤ情報を上記所定の装置に送信する送信手段とを備えたことを特徴とするリモ

ートアクセス実行装置。

【請求項１８】　上記位置情報取得手段は、ＧＰＳ受信機により上記第１の位置情報を取得することを特徴とする請求項１７に記載のリモートアクセス実行装置。

【請求項１９】　上記ＩＤ情報取得手段は、自機の所定個所或いは自機に使用される部材の所定個所に書き込まれたＩＤを読み取って取得することを特徴とする請求項１７に記載のリモートアクセス実行装置。

【請求項２０】　所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の第１の位置情報、及び上記所定の装置の第２の位置情報が予め組み合わされているＩＤ情報を受信する受信手段と、

上記第１の位置情報と上記ＩＤ情報に組み合わされている上記第２の位置情報とを照合する照合手段とを備えたことを特徴とするリモートアクセス実行装置。

【請求項２１】　上記照合手段により第１の位置情報と上記ＩＤ情報に組み合わされている上記第２の位置情報とが異なると判断された場合、リモートアクセスを切断するリモートアクセス切断手段を備えたことを特徴とする請求項２０に記載のリモートアクセス実行装置。

【請求項２２】　上記照合手段は、上記所定の装置との間のリモートアクセス中に繰り返し照合を行うことを特徴とする請求項２０又は２１に記載のリモートアクセス実行装置。

【請求項２３】　所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、

自機の位置情報を取得する位置情報取得手順と、

上記所定の装置との間のリモートアクセス時に、上記位置情報取得手順により取得された上記位置情報を上記所定の装置に送信する送信手順とを行うことを特徴とするリモートアクセス実行方法。

【請求項２４】　所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の位置情報を受信する受信処理と、

上記受信処理により受信された上記位置情報が所定範囲内にあるか否かを照合する照合処理とを行うことを特徴とするリモートアクセス実行方法。

【請求項２５】　所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、

自機のＩＤ情報を取得するＩＤ情報取得処理と、

上記所定の装置との間のリモートアクセス時に、上記ＩＤ情報取得処理により取得された上記ＩＤ情報を上記所定の装置に送信する送信処理とを行うことを特徴とするリモートアクセス実行方法。

【請求項２６】　所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置のＩＤ情報を受信する受信処理と、

上記受信処理により受信された上記ＩＤ情報によるＩＤが所定ＩＤであるか否かを照合する照合処理とを行うことを特徴とするリモートアクセス実行方法。

【請求項２７】　所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、

自機の第１の位置情報を取得する位置情報取得処理と、

自機の第２の位置情報が予め組み合わされているＩＤ情報を取得するＩＤ情報取得処理と、

上記所定の装置との間のリモートアクセス時に、上記第１の位置情報及び上記ＩＤ情報を上記所定の装置に送信する送信処理とを行うことを特徴とするリモートアクセス実行方法。

【請求項２８】　所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の第１の位置情報、及び上記所定の装置の第２の位置情報が予め組み合わされているＩＤ情報を受信する受信処理と、

上記第１の位置情報と上記ＩＤ情報に組み合わされている上記第２の位置情報とを照合する照合処理とを行うことを特徴とするリモートアクセス実行方法。

【請求項２９】　所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、

自機の位置情報を取得する位置情報取得手順と、

上記所定の装置との間のリモートアクセス時に、上記位置情報取得手順により取得された上記位置情報を上記所定の装置に送信する送信手順とを実行するプログラムを格納したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項３０】　所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の位置情報を受信する受信処理と、

上記受信処理により受信された上記位置情報が所定範囲内にあるか否かを照合する照合処理とを実行するプログラムを格納したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項３１】　所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、

自機のＩＤ情報を取得するＩＤ情報取得処理と、

上記所定の装置との間のリモートアクセス時に、上記ＩＤ情報取得処理により取得された上記ＩＤ情報を上記所定の装置に送信する送信処理とを実行するプログラムを格納したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項３２】　所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置のＩＤ情報を受信する受信処理と、

上記受信処理により受信された上記ＩＤ情報によるＩＤが所定ＩＤであるか否かを照合する照合処理とを実行するプログラムを格納したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項３３】　所定の装置との間でリモートアクセスを行うためのプログ

ラムを格納したコンピュータ読み取り可能な記憶媒体であって、

自機の第１の位置情報を取得する位置情報取得処理と、

自機の第２の位置情報が予め組み合わされている自機のＩＤ情報を取得するＩＤ情報取得処理と、

上記所定の装置との間のリモートアクセス時に、上記第１の位置情報及び上記ＩＤ情報を上記所定の装置に送信する送信処理とを実行するプログラムを格納したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項３４】　所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の第１の位置情報、及び上記所定の装置の第２の位置情報が予め組み合わされているＩＤ情報を受信する受信処理と、

上記第１の位置情報と上記ＩＤ情報に組み合わされている上記第２の位置情報とを照合する照合処理とを実行するプログラムを格納したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークシステム、リモートアクセス実行装置、方法、及びコンピュータ読み取り可能な記憶媒体に関し、特に世界にまたがるネットワーク構築や世界規模で散在する半導体製造工場等において使用される装置のリモート保守管理等のリモートアクセス時における不正アクセスを防止するのに適する。

【０００２】

【従来の技術】

近年、一般のパーソナルコンピュータはもちろんのこと、特定業務向けの装置（半導体製造装置等）、或いはモバイル端末のようなものも、ネットワーク技術の進歩により公衆回線を用いたリモートアクセスが簡単に実現できるようになっている。リモートアクセス技術を用いることにより、例えば、通信回線経由で最新のソフトウェアをダウンロードしてすぐに利用したり、或いは、特定業務向け

の装置であれば２４時間の遠隔保守により不具合の調査や修正をサービスマンが赴くことなくタイムリーに実現したり、或いは、装置パラメータの調整をサービスマンが装置設置場所に赴くことなく実現したりする等の、様々な応用が実現可能となっている。

【０００３】

ところが、近年、ネットワーク社会の発達、普及に伴って、パスワードの盗用・ハッキングにより、悪意のある第三者がコンピュータネットワークに侵入し、データの改ざんや消去、機密データへのアクセス、顧客情報データの漏洩等の深刻な被害を受ける例が後を絶たないようになってきている。

【０００４】

このようなネットワークの不正アクセスによる被害を防止するために、従来から種々の方法が提案されている。例えば、アクセス許可されている電話番号に対してリモートアクセス先から接続しなおすコールバック方式や、アクセス許可電話番号の発信者番号通知を用いて、アクセス許可電話番号のリストに該当するものがない場合には接続不可能とする方式や、リモートアクセスのクライアントとサーバ側とでカウンタ同期方式やＡＮＳＩ規格準拠のチャレンジ・レスポンス方式によりワンタイムパスワード生成器（接続のたびにパスワードを発生させる方式）を用いてアクセス許可を行う方式等がある。

【０００５】

【発明が解決しようとする課題】

しかしながら、インターネット等で流通するネットワークハッキング・クラッキング用のソフトウェアは年々高度な技術を持つハッカーの手により強力なものとなってきており、セキュリティの高いといわれてきた方式でも昨今では破られるようになっている。このため、不正アクセスに対する抜本的な対策を行うために、原理的或いは物理的に絶対にクラッキング不可能な不正アクセス防止方式が提供されることが必要とされている。

【０００６】

本発明は、上記のような実情に鑑みてなされたものであり、不正アクセスを確実に防止できるようにすることを目的とする。

【０００７】

【課題を解決するための手段】

本発明のネットワークシステムは、所定の装置間でのリモートアクセスを可能としたネットワークシステムであって、上記所定の装置のうち一方の装置は、自機の位置情報を取得する位置情報取得手段と、上記位置情報取得手段により取得された上記位置情報を送信する送信手段を備え、上記所定の装置のうち他方の装置は、上記送信手段により送信された上記位置情報を受信する受信手段と、上記受信手段により受信された上記位置情報が所定範囲内にあるか否かを照合する照合手段とを備える点に特徴を有する。

【０００８】

本発明のリモートアクセス実行装置は、所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、自機の位置情報を取得する位置情報取得手段と、上記所定の装置との間のリモートアクセス時に、上記位置情報取得手段により取得された上記位置情報を上記所定の装置に送信する送信手段とを備えた点に特徴を有する。

【０００９】

本発明のリモートアクセス実行装置は、所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の位置情報を受信する受信手段と、上記受信手段により受信された上記位置情報が所定範囲内にあるか否かを照合する照合手段とを備えた点に特徴を有する。

【００１０】

また、本発明のネットワークシステムは、所定の装置間でのリモートアクセスを可能としたネットワークシステムであって、上記所定の装置のうち一方の装置は、自機のＩＤ情報を取得するＩＤ情報取得手段と、上記ＩＤ取得手段により取得された上記ＩＤ情報を送信する送信手段を備え、上記所定の装置のうち他方の装置は、上記送信手段により送信された上記ＩＤ情報を受信する受信手段と、上記受信手段により受信された上記ＩＤ情報によるＩＤが所定ＩＤであるか否かを照合する照合手段とを備える点に特徴を有する。

【００１１】

本発明のリモートアクセス実行装置は、所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、自機のＩＤ情報を取得するＩＤ情報取得手段と、上記所定の装置との間のリモートアクセス時に、上記ＩＤ情報取得手段により取得された上記ＩＤ情報を上記所定の装置に送信する送信手段とを備えた点に特徴を有する。

【００１２】

本発明のリモートアクセス実行装置は、所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置のＩＤ情報を受信する受信手段と、上記受信手段により受信された上記ＩＤ情報によるＩＤが所定ＩＤであるか否かを照合する照合手段とを備えた点に特徴を有する。

【００１３】

また、本発明のネットワークシステムは、所定の装置間でのリモートアクセスを可能としたネットワークシステムであって、上記所定の装置のうち一方の装置は、自機の第１の位置情報を取得する位置情報取得手段と、自機の第２の位置情報が予め組み合わされているＩＤ情報を取得するＩＤ情報取得手段と、上記第１の位置情報及び上記ＩＤ情報を送信する送信手段を備え、上記所定の装置のうち他方の装置は、上記送信手段により送信された上記第１の位置情報及び上記ＩＤ情報を受信する受信手段と、上記第１の位置情報と上記ＩＤ情報に組み合わされている上記第２の位置情報とを照合する照合手段とを備える点に特徴を有する。

【００１４】

本発明のリモートアクセス実行装置は、所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、自機の第１の位置情報を取得する位置情報取得手段と、自機の第２の位置情報が予め組み合わされているＩＤ情報を取得するＩＤ情報取得手段と、上記所定の装置との間のリモートアクセス時に、上記第１の位置情報及び上記ＩＤ情報を上記所定の装置に送信する送信手段とを備えた点に特徴を有する。

【００１５】

本発明のリモートアクセス実行装置は、所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の第１の位置情報、及び上記所定の装置の第２の位置情報が予め組み合わされているＩＤ情報を受信する受信手段と、上記第１の位置情報と上記ＩＤ情報に組み合わされている上記第２の位置情報とを照合する照合手段とを備えた点に特徴を有する。

【００１６】

本発明のリモートアクセス実行方法は、所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、自機の位置情報を取得する位置情報取得手順と、上記所定の装置との間のリモートアクセス時に、上記位置情報取得手順により取得された上記位置情報を上記所定の装置に送信する送信手順とを行う点に特徴を有する。

【００１７】

本発明のリモートアクセス実行方法は、所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の位置情報を受信する受信処理と、上記受信処理により受信された上記位置情報が所定範囲内にあるか否かを照合する照合処理とを行う点に特徴を有する。

【００１８】

本発明のリモートアクセス実行方法は、所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、自機のＩＤ情報を取得するＩＤ情報取得処理と、上記所定の装置との間のリモートアクセス時に、上記ＩＤ情報取得処理により取得された上記ＩＤ情報を上記所定の装置に送信する送信処理とを行う点に特徴を有する。

【００１９】

本発明のリモートアクセス実行方法は、所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置のＩＤ情報を受信する受信処理と、上記受信処理により受信された上記ＩＤ情報によるＩＤが所定ＩＤであるか否かを照合する照合

処理とを行う点に特徴を有する。

【００２０】

本発明のリモートアクセス実行方法は、所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、自機の第１の位置情報を取得する位置情報取得処理と、自機の第２の位置情報が予め組み合わされているＩＤ情報を取得するＩＤ情報取得処理と、上記所定の装置との間のリモートアクセス時に、上記第１の位置情報及び上記ＩＤ情報を上記所定の装置に送信する送信処理とを行う点に特徴を有する。

【００２１】

本発明のリモートアクセス実行方法は、所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の第１の位置情報、及び上記所定の装置の第２の位置情報が予め組み合わされているＩＤ情報を受信する受信処理と、上記第１の位置情報と上記ＩＤ情報に組み合わされている上記第２の位置情報とを照合する照合処理とを行う点に特徴を有する。

【００２２】

本発明のコンピュータ読み取り可能な記憶媒体は、所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、自機の位置情報を取得する位置情報取得手順と、上記所定の装置との間のリモートアクセス時に、上記位置情報取得手順により取得された上記位置情報を上記所定の装置に送信する送信手順とを実行するプログラムを格納した点に特徴を有する。

【００２３】

本発明のコンピュータ読み取り可能な記憶媒体は、所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の位置情報を受信する受信処理と、上記受信処理により受信された上記位置情報が所定範囲内にあるか否かを照合する照合処理とを実行するプログラムを格納した点に特徴を有する。

【００２４】

本発明のコンピュータ読み取り可能な記憶媒体は、所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、自機のＩＤ情報を取得するＩＤ情報取得処理と、上記所定の装置との間のリモートアクセス時に、上記ＩＤ情報取得処理により取得された上記ＩＤ情報を上記所定の装置に送信する送信処理とを実行するプログラムを格納した点に特徴を有する。

【００２５】

本発明のコンピュータ読み取り可能な記憶媒体は、所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置のＩＤ情報を受信する受信処理と、上記受信処理により受信された上記ＩＤ情報によるＩＤが所定ＩＤであるか否かを照合する照合処理とを実行するプログラムを格納した点に特徴を有する。

【００２６】

本発明のコンピュータ読み取り可能な記憶媒体は、所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、自機の第１の位置情報を取得する位置情報取得処理と、自機の第２の位置情報が予め組み合わされている自機のＩＤ情報を取得するＩＤ情報取得処理と、上記所定の装置との間のリモートアクセス時に、上記第１の位置情報及び上記ＩＤ情報を上記所定の装置に送信する送信処理とを実行するプログラムを格納した点に特徴を有する。

【００２７】

本発明のコンピュータ読み取り可能な記憶媒体は、所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の第１の位置情報、及び上記所定の装置の第２の位置情報が予め組み合わされているＩＤ情報を受信する受信処理と、上記第１の位置情報と上記ＩＤ情報に組み合わされている上記第２の位置情報とを照合する照合処理とを実行するプログラ

ムを格納した点に特徴を有する。

【００２８】

【発明の実施の形態】

以下、図面を参照して、本発明のリモートアクセス管理システム、リモートアクセス管理装置、方法、及びコンピュータ読み取り可能な記憶媒体の実施の形態について説明する。本実施の形態では、本発明を適用する例として、地理的に離れた拠点に設置される装置として、ステッパー（光縮小投影露光装置）等の半導体露光装置について説明する。そして、サーバ機１５０等との間でリモートアクセスを行うことにより、リモート保守等のサービスが実現されるようにしている。

【００２９】

（第１の実施の形態）

図１には、半導体露光装置のハードウェアシステム構成を示す。１０１はコンソール用ＣＰＵであり、半導体露光装置のコンソール表示とコンソールコマンド入力による操作の制御を司る。１０２はＲＡＭであり、ＣＰＵ１０１が実行プログラムを格納したりデータを格納したりする。１０３はＲＯＭであり、プログラムを格納する。

【００３０】

１０４は補助記憶装置であり、データ及びプログラムを格納するために用いられる。通常、ソフトウェアプログラムは、この補助記憶装置１０４に保存される。ソフトウェアプログラムは、一般にファイルシステムを補助記憶装置１０４上に構成しファイルとして管理する。補助記憶装置１０４としては、ハードディスク等の磁気ディスク装置を用いることが多いが、装置構成や露光作業の性質、運用の違いに応じて、フラッシュメモリやＮＶ－ＲＡＭ（不揮発性メモリ）、ＥＥＰ－ＲＯＭといったソフトウェア的な書き換え可能な部品を用いることもある。

【００３１】

１０６はＧＰＳ用インターフェースであり、後述するＧＰＳ受信機１０８と通信を行う。ＧＰＳ用インターフェース１０６としては、一般にＲＳ２３２Ｃ等のシリアル通信インターフェースを用いることが多いが、ＧＰＳ通信におけるデー

タ量によってはパラレルインターフェースやＳＣＳＩインターフェース等を用いてもかまわない。また、ＧＰＳ用インターフェース１０６とＧＰＳ受信機１０８との間で行う通信のプロトコルとして、一般に無手順非同期方式を用いるが、同期式やバイナリ手順を採用してもかまわない。

【００３２】

１０５はコンソール装置であり、オペレータ（操作者）は本装置１０５よりコンソール用ＣＰＵ１０１に対する指令を行うことができる。コンソール装置１０５の表示装置としては、ＣＲＴや液晶表示装置、ＥＬパネル、或いはプラズマディスプレイ等を用いる。また、コンソール装置１０５の入力装置としては、コマンドをキー入力するためのキーボードを用いることが多いが、電子ペンによるペン入力装置（タブレット）やタッチパネル等で構成されることもある。

【００３３】

１０８はＧＰＳ（Global Positioning System）受信機であり、衛星からのＧＰＳ電波を受信するためのＧＰＳアンテナからＧＰＳ電波内のディジタル信号を復号（デコード）し、半導体露光装置が設置されている緯度経度情報（位置情報）や時刻情報を取得する。ＧＰＳアンテナは、装置がクリーンルーム等の電波の届かない所にある場合、電波の届く外部まで電線を延長して敷設することも可能である。

【００３４】

１０９は通信インターフェースであり、外部通信網（公衆電話回線網等）と通信を行う通信装置１１６と通信を行ってリモートアクセスを実現する。通信インターフェース１０９としては、一般にＲＳ２３２Ｃ等のシリアル通信インターフェースを用いる場合が多いが、パラレルインターフェースやＵＳＢ等の高速インターフェースを用いることも多くなっている。

【００３５】

１１６は通信装置であり、公衆回線等の通信網１１７を用いて遠隔の装置（サーバ機１５０等）とのリモートアクセスを実現する。通信装置１１６としては、通信網１１７がアナログ公衆回線等の場合にはモデム等の装置を用いるが、通信網１１７がＩＳＤＮ等のディジタル公衆回線等であったり、ディジタル専用線で

あったりする場合にはディジタル通信用のターミナルアダプタ（ＴＡ）等を用いる。或いは、ＰＨＳや携帯電話用のディジタル通信であれば、ＰＨＳや携帯電話用のディジタル通信カードを用いることもある。

【００３６】

上記通信インターフェース１０９及び通信装置１１６を用いてリモートアクセスを可能とするための通信プロトコルには、一般にＴＣＰ／ＩＰによるポイント・トゥー・ポイント接続（ＰＰＰ接続）等を用いるが、リモートアクセスを実現できるプロトコルであれば、アップルトークやネットウェア、或いはパソコン通信等で用いられるベーシック手順等を用いて実現してもかまわない。

【００３７】

１１０はメインＣＰＵであり、半導体露光装置を構成する各種の制御装置を全体制御する。当該メインＣＰＵ１１０と上記コンソール用ＣＰＵ１０１とは、メインＣＰＵバス１０７により接続され、半導体露光装置として動作する。

【００３８】

１１１は照明装置であり、半導体製造用のウェハに対して露光する光源を制御するためのものである。１１２はレチクル駆動装置であり、半導体製造用のウェハに対して露光するパターンを描いたレチクル（フォトマスク）の搬入搬出等を制御するためのものである。１１３はステージ駆動装置であり、半導体製造用のウェハをステップアンドリピートの方式で露光するためにＸＹステージ上等でウェハを駆動制御するためのものである。１１４はアライメント用ＴＶシステムであり、半導体製造用のウェハの正確な位置決めをして制御するためのものである。　これら各装置１１１～１１４は、周辺機器用バス１１５によりメインＣＰＵ１１０の制御下におかれる。本実施の形態では、周辺機器用バス１１５としてＳＣＳＩを用いるが、どのような汎用の標準バスで構成されていてもかまわない。

【００３９】

次に、図２のフローチャートに基づいて、第１の実施の形態における不正アクセス防止のための処理動作について説明する。前提として、リモートアクセスを許可したユーザからは、当該ユーザの半導体露光装置の設置場所の緯度経度情報を予め取得しておく。そして、半導体露光装置との間でリモートアクセスを行う

サーバ機１５０等には、上記予め取得した半導体露光装置の設置場所の緯度経度情報と、許容される緯度経度のオフセット範囲（どれくらいの距離の移動を許容するかという範囲）の情報とのリストを記憶させておく。

【００４０】

図２のフローチャートに示すプログラムルーチンは、半導体露光装置とサーバ機１５０等との間でのリモートアクセスが開始されると実行され、また、リモートアクセス中に一定の基準で何度も繰り返し実行される。

【００４１】

半導体露光装置では、半導体露光装置に埋め込まれているＧＰＳ受信機１０８により、当該半導体露光装置が現在設置されている場所の緯度経度情報が取得される（ステップ２０１）。そして、このＧＰＳ受信データ（緯度経度情報）は、通信インターフェース１０９及び通信装置１１６を介してリモートアクセスの相手であるサーバ機１５０等へ送出される（ステップ２０２）。

【００４２】

サーバ機１５０等では、半導体露光装置から上記ＧＰＳ受信データを受信して、そのＧＰＳ受信データによる装置設置場所の緯度経度情報を、許容される緯度経度のオフセット範囲を加算して算出したリモートアクセスを許可すべきユーザ装置設置場所の緯度経度情報と比較・照合する（ステップ２０３）。そして、上記比較・照合した結果、上記ＧＰＳ受信データによる装置設置場所の緯度経度情報がオフセット範囲からずれているような場合には、不正な設置場所データ、或いは改ざん、偽造による無効なＧＰＳ受信データであると判断し（ステップ２０４）、ステップ２０５に移行してリモートアクセスを切断する。

【００４３】

以上述べた動作により、リモートアクセスを許可した半導体露光装置の設置場所以外の場所からの不正アクセスを防止することができる。特に、半導体露光装置等では、リモートアクセスが全世界的に配置されている拠点間のリモート保守等のネットワーク接続に利用される場合が多いので、本実施の形態における不正リモートアクセス防止方式は有効である。なお、実際の運用においては、本実施の形態で述べた方式と、従来の方式、例えばコールバック方式、着信電話番号を

照合する方式、或いはワンタイムパスワード方式等を併用してもよい。

【００４４】

（第２の実施の形態）

上記第１の実施の形態では、ＧＰＳ受信機１０８により取得した半導体露光装置の緯度経度情報を送信することにより不正アクセスを防止するようにしたが、本第２の実施の形態では、半導体露光装置の光学系部品或いは媒体に書き込まれた装置固有のＩＤを送信することにより不正アクセスを防止する。

【００４５】

第２の実施の形態における半導体露光装置のハードウェアシステムの基本的な構成は、図１で説明したのと同様であるが、ＧＰＳ受信機１０８やＧＰＳ用インターフェース１０６は必要ではなく、装置固有のＩＤを読み取るためのＩＤ読み取り手段が必要となる。

【００４６】

半導体露光装置では、メインＣＰＵ１１０からの指示によって、照明装置１１１等を動作させ、各装置、例えばレチクル駆動装置１１２であれば、レチクルに書き込まれた装置固有のＩＤを読み取って、周辺機器用バス１１５に当該ＩＤのデータを送出し、メインＣＰＵ１１０へＩＤのデータを受け渡す。

【００４７】

上記ＩＤのデータはメインＣＰＵ１１０からＲＡＭ１０２に書き込まれ、コンソール用ＣＰＵ１０１の指令により通信インターフェース１０９及び通信装置１１６に渡されて、通信網１１７を介してリモートアクセスの相手であるサーバ機１５０等へ送出される。上記ＩＤのデータは、例えばＡＳＣＩＩテキストのようなデータであってもよいが、レチクルに書き込む際になんらかの暗号化を施しておき、上記暗号化されているデータのまま送出し、リモートアクセスの相手であるサーバ機１５０等で管理されている秘密鍵を用いて復号するような実施の形態が望ましい。

【００４８】

図３には、半導体露光装置の模式図を示す。図３において、３０１は照明装置１１１の露光光源、３０２は露光量制御のためのシャッタ、３０３は回路パター

ンの原板となるレチクル、３０４はレチクル３０３を保持するためのレチクルステージ、３０５はレチクル３０３を搬入するためのレチクルハンドである。

【００４９】

また、３０６は投影レンズ、３０７は半導体基盤であるウェハ、３０８はウェハ３０７を保持し、露光光源３０１とのフォーカスを合わせるためのウェハＺステージ、３０９はウェハＺステージ３０８をＸＹ方向へ移動させるためのＸＹステージ、３１０はＸＹステージ３０９の位置を計測するためのレーザ干渉計、３１１は露光処理をするためのウェハ３０７をウェハＺステージ３０８へ供給するためのウェハ供給ハンド、３１２は露光処理を終えたウェハ３０７をウェハＺステージ３０８から回収するためのウェハ回収ハンドである。

【００５０】

図３に示した半導体露光装置等の光学機器には、レチクル３０３やレチクルステージ３０４、或いはウェハＺステージ３０８やＸＹステージ３０９といった特殊な部品を具備している。レチクル３０３やステージ３０４、３０８、３０９等には、レチクルやウェハの位置合わせを行うためのレチクルセットマークやレチクル基準マーク、ステージ基準マーク、ＴＴＬ－ＡＦ基準マーク或いはウェハ基準マークといったマイクロメータ単位の微小なパターンマーク図形が書き込まれており、これらパターンやマークの読み取りには微小パターンを読み取るための各種の特殊な光学系スコープを用いる。

【００５１】

本実施の形態では、上記パターンやマークとして、装置固有のＩＤをテストレチクルやテストウェハ、或いは半永久的に交換する可能性のないステージ等に微小パターンとして書き込み、当該ＩＤを上記光学系スコープにより読み取る手段を具備することによってＩＤを生成する。

【００５２】

ＩＤを生成するのに特殊な光学系デバイスと光学系読み取り装置とを必要とし、かつ上記読み取り手段をリモートアクセス時に必ず実行しなければＩＤを取得できない構成となるため、ＩＤの偽造や改ざん、或いはＩＤの読み取り手段のバイパスによる不正アクセスに対して強力な防衛手段となる。

【００５３】

レチクル等の光学部品に書き込まれた文字パターン等のデータは、上記光学系スコープにより読み取ったディジタル画像から文字認識を行い、文字データとして取得するのが望ましい。上記文字データは、装置の製造シリアル番号等をそのままＡＳＣＩＩコード等で記述したものをＩＤとして利用してもよいが、装置の製造シリアル番号等を秘密鍵によって暗号化した文字データをレチクル等の特殊光学系部品に書き込み、上記暗号化されたＩＤの復号は、リモートアクセスの相手であるサーバ機１５０等の上で管理されている秘密鍵を用いて復号し、リモートアクセスの許可されているＩＤのリストとの照合を行う構成とすることが望ましい。

【００５４】

次に、図４のフローチャートに基づいて、第２の実施の形態における不正アクセス防止のための処理動作について説明する。前提として、半導体露光装置との間でリモートアクセスを行うサーバ機１５０等には、リモートアクセスを許可するＩＤのリストを記憶させておく。

【００５５】

図４のフローチャートに示すプログラムルーチンは、半導体露光装置とサーバ機１５０等との間でのリモートアクセスが開始されると実行され、また、リモートアクセス中に一定の基準で何度も繰り返し実行される。

【００５６】

半導体露光装置では、レチクル等の特殊な光学系部品に書き込まれた装置固有のＩＤが取得される（ステップ４０１）。そして、このＩＤのデータは、通信インターフェース１０９及び通信装置１１６を介してリモートアクセスの相手であるサーバ機１５０等へ送出される（ステップ４０２）。

【００５７】

サーバ機１５０等では、半導体露光装置から上記ＩＤのデータを受信して、そのＩＤが、リモートアクセスを許可するＩＤのリストにあるか否かを比較・照合する（ステップ４０３）。そして、上記比較・照合した結果、リストにないような場合には、不正なＩＤであると判断し（ステップ４０４）、ステップ４０５に

移行してリモートアクセスを切断する。

【００５８】

以上述べた動作により、リモートアクセスを許可したＩＤを取得できない半導体露光装置からの不正アクセスを防止することができる。ＩＤを特殊な光学系部品からスコープ等の特殊な光学系装置で読み取る手段は、リモートアクセス中に、一定の基準で随時行われるようにリモートアクセス用のプログラム内に埋め込まれている。すなわち、リモートアクセス用のプログラム動作中は、必ず読み取り手段が動作してＩＤを読み取るので、本実施の形態における不正アクセス防止方式を回避してリモートアクセスすることは非常に困難であるといえる。

【００５９】

また、上述したように、リモートアクセスの相手であるサーバ機１５０等で管理している秘密鍵を用いて暗号化したＩＤをレチクル等の特殊な光学系部品に書き込むようにすることで、通信プロトコル上に送出されるＩＤは暗号化されたものとなり、セキュリティレベルの向上を図ることが可能となる。

【００６０】

従来は、装置固有のＩＤや前述のワンタイムパスワード方式の秘密鍵の保持方式としては、半導体で作られた記憶素子（メモリ）に書き込んで保持するものであったが、本実施の形態では、物理的、光学的に特殊な特性を有する部品或いは媒体にＩＤや秘密鍵等を書き込み、それを光学的に読み取るようにしたので、高度な技術を持つハッカーでもＩＤ等の偽造が原理的に困難であり、不正アクセスを有効に防止することが可能となる。

【００６１】

（第３の実施の形態）

第３の実施の形態では、上記第１の実施の形態で説明したようにＧＰＳ受信機１０８により取得した緯度経度情報と、上記第２の実施の形態で説明したように半導体露光装置の光学系部品或いは媒体に書き込まれた装置固有のＩＤとを、リモートアクセスの相手であるサーバ機１５０等に送信することにより不正アクセスを防止するようにしている。さらに、ＩＤとして、装置設置場所情報を組み合わせた複合ＩＤを用いることにより、多段階の不正アクセス防止方式を提供する

ことができ、より確実に不正アクセスを防止することができる。

【００６２】

図５のフローチャートに基づいて、第３の実施の形態における不正アクセス防止のための処理動作について説明する。図５のフローチャートに示すプログラムルーチンは、半導体露光装置とサーバ機１５０等との間でのリモートアクセスが開始されると実行され、また、リモートアクセス中に一定の基準で何度も繰り返し実行される。

【００６３】

半導体露光装置では、半導体露光装置に埋め込まれているＧＰＳ受信機１０８により、当該半導体露光装置が現在設置されている場所の緯度経度情報が取得される（ステップ５０１）。また、レチクル等の特殊な光学系部品に書き込まれた装置固有の製造シリアル番号等と装置設置場所情報を組み合わせた複合ＩＤが取得される（ステップ５０２）。そして、ＧＰＳ受信データ（緯度経度情報）と複合ＩＤのデータとは、通信インターフェース１０９及び通信装置１１６を介してリモートアクセスの相手であるサーバ機１５０等へ送出される（ステップ５０３）。

【００６４】

サーバ機１５０等では、半導体露光装置からの上記ＧＰＳ受信データ及び上記複合ＩＤのデータを受信して、そのＧＰＳ受信データによる装置設置場所の緯度経度情報を、許容される緯度経度のオフセット範囲を加算して算出したリモートアクセスを許可すべきユーザ装置設置場所の緯度経度情報と比較・照合する（ステップ５０４）。また、その複合ＩＤが、リモートアクセスを許可するＩＤのリストにあるか否かを比較・照合する（ステップ５０６）。

【００６５】

そして、上記比較・照合した結果、半導体露光装置の現在設置されている場所の緯度経度情報がオフセット範囲からずれているような場合には、不正な設置場所データ、或いは改ざん、偽造による無効なＧＰＳ受信データであると判断し（ステップ５０８）、ステップ５１１に移行してリモートアクセスを切断する。同様に、リモートアクセスを許可するＩＤのリストにないような場合には、不正な

ＩＤであると判断し（ステップ５０９）、ステップ５１１に移行してリモートアクセスを切断する。さらに、上記複合ＩＤ上の装置設置場所情報と、上記ＧＰＳ受信データによる緯度経度情報とに相違があれば（ステップ５１０）、ステップ５１１に移行してリモートアクセスを切断する。

【００６６】

以上述べた動作により、上記第１、２の実施の形態で述べた効果が得られるとともに、ＩＤとして、装置設置場所情報を組み合わせた複合ＩＤを用いることにより、多段階の不正アクセス防止方式を提供することができ、より確実に不正アクセスを防止することができる。

【００６７】

なお、図１に示したＧＰＳ受信機１０８と装置とのインターフェースを装置の内部に埋め込むことなく、ＬＡＮ等のネットワークによる通信網を介して、ＧＰＳ受信機１０８よりのデータを送信する実施の形態も実現可能である。例えば、半導体露光装置がクリーンルームに設置されており、装置に埋め込まれたＧＰＳ受信機からアンテナをＧＰＳ電波の受信可能な場所まで敷設することが困難な場合に効果的である。

【００６８】

ただし、本方式ではネットワークとの通信インターフェースがＧＰＳ受信機１０８と装置との間に介在するため、ネットワークパケット内容の改ざんや暗号の解読により、本方式による違法コピー防止方式が破られてしまうおそれがある。最も強力な実施の形態は、装置内部にＧＰＳ受信機１０８と装置との切り離し不可能なインターフェースを確保する形態である。

【００６９】

（その他の実施の形態）

上述した実施の形態の機能を実現するべく各種のデバイスを動作させるように、該各種デバイスと接続された装置或いはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステム或いは装置のコンピュータ（ＣＰＵ或いはＭＰＵ）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも

、本発明の範疇に含まれる。

【００７０】

また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００７１】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）或いは他のアプリケーションソフト等と共同して上述の実施の形態の機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることはいうまでもない。

【００７２】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部又は全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれることはいうまでもない。

【００７３】

なお、上記実施の形態において示した各部の形状及び構造は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

【００７４】

【発明の効果】

以上述べたように本発明によれば、リモートアクセスを許可した装置設置場所以外からのリモートアクセスや、リモートアクセスを許可するＩＤを持たない装置からのリモートアクセスを発見することができ、不正アクセスを防止することが可能となる。

【図面の簡単な説明】

【図１】

半導体露光装置のハードウェア構成を示す図である。

【図２】

第１の実施の形態における処理動作を示すフローチャートである。

【図３】

半導体露光装置の模式図である。

【図４】

第２の実施の形態における処理動作を示すフローチャートである。

【図５】

第３の実施の形態における処理動作を示すフローチャートである。

【符号の説明】

１０１　コンソール用ＣＰＵ

１０２　ＲＡＭ

１０３　ＲＯＭ

１０４　補助記憶装置

１０５　コンソール装置

１０６　ＧＰＳ用インターフェース

１０７　メインＣＰＵバス

１０８　ＧＰＳ受信機

１０９　通信インターフェース

１１０　メインＣＰＵ

１１１　照明装置

１１２　レチクル駆動装置

１１３　ステージ駆動装置

１１４　ＴＶシステム

１１５　周辺機器用バス

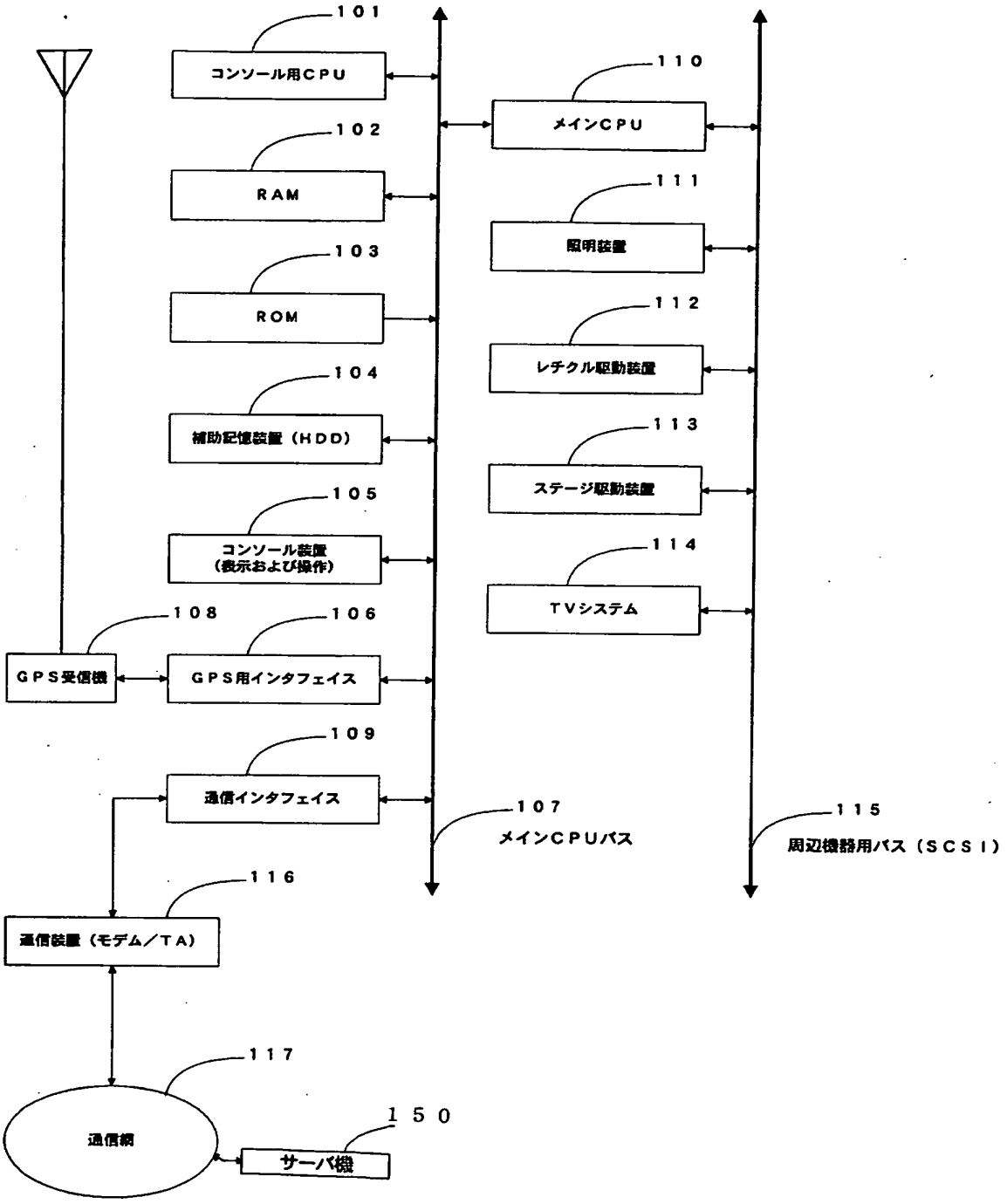
１１６　通信装置

１１７　通信網

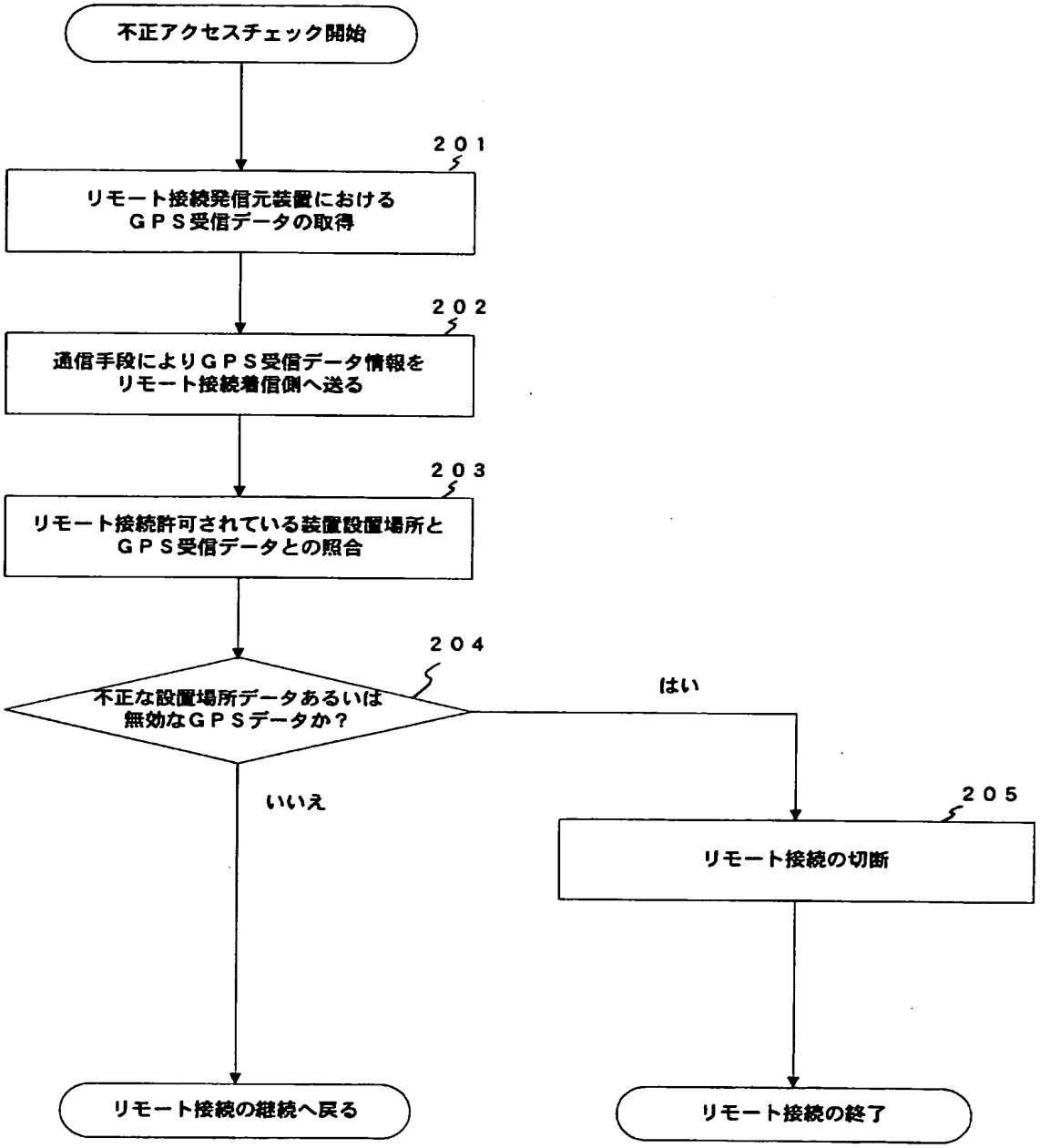
１５０　サーバ機

【書類名】　　図面

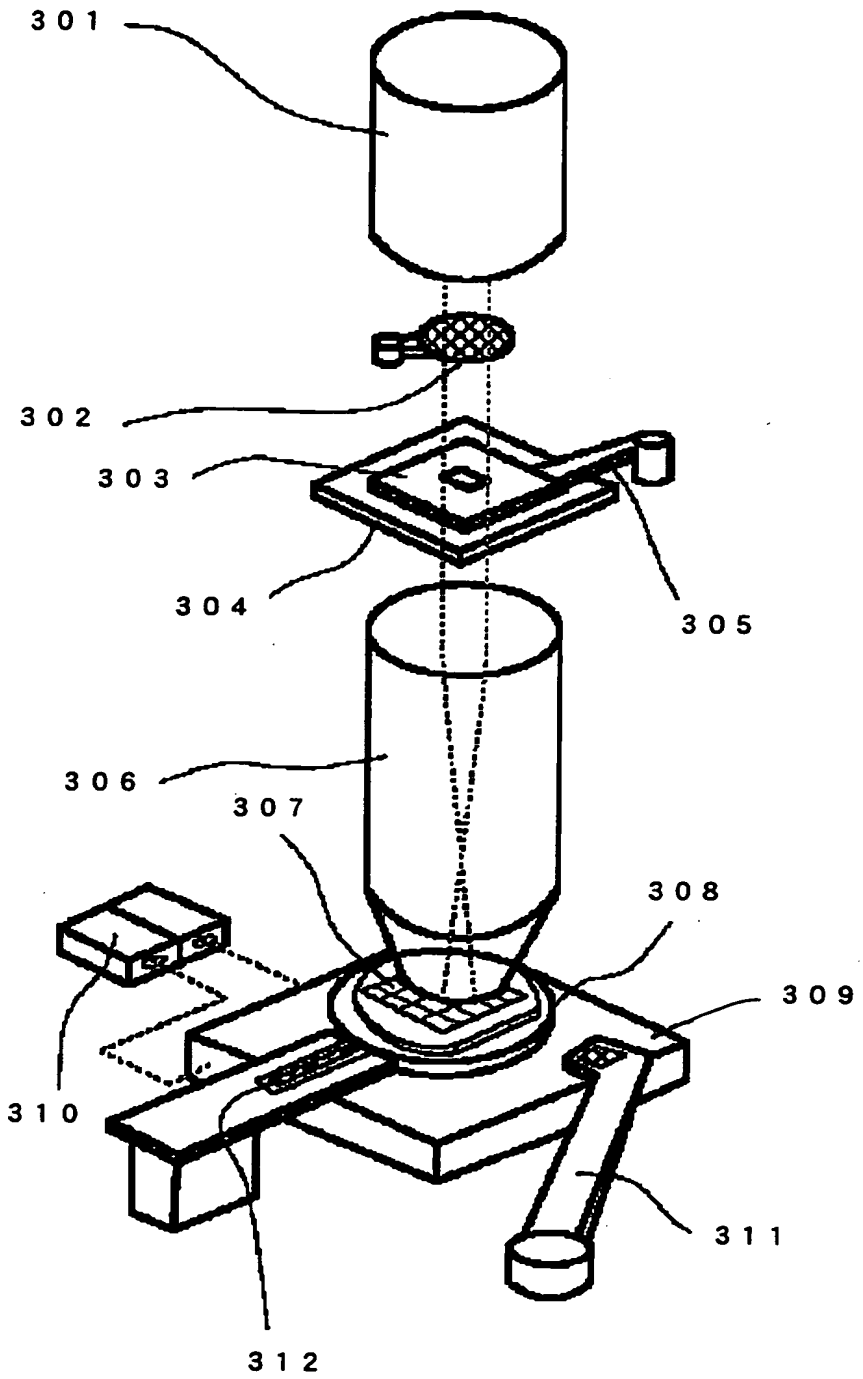
【図１】


101
コンソール用CPU
102
RAM
103
ROM
104
補助記憶装置（HDD）
105
コンソール装置
（表示および操作）
108
GPS受信機
106
GPS用インタフェイス
109
通信インタフェイス
107
メインCPUバス
110
メインCPU
111
照明装置
112
レチクル駆動装置
113
ステージ駆動装置
114
TVシステム
115
周辺機器用バス（SCSI）
116
通信装置（モデム／TA）
117
通信網
150
サーバ機

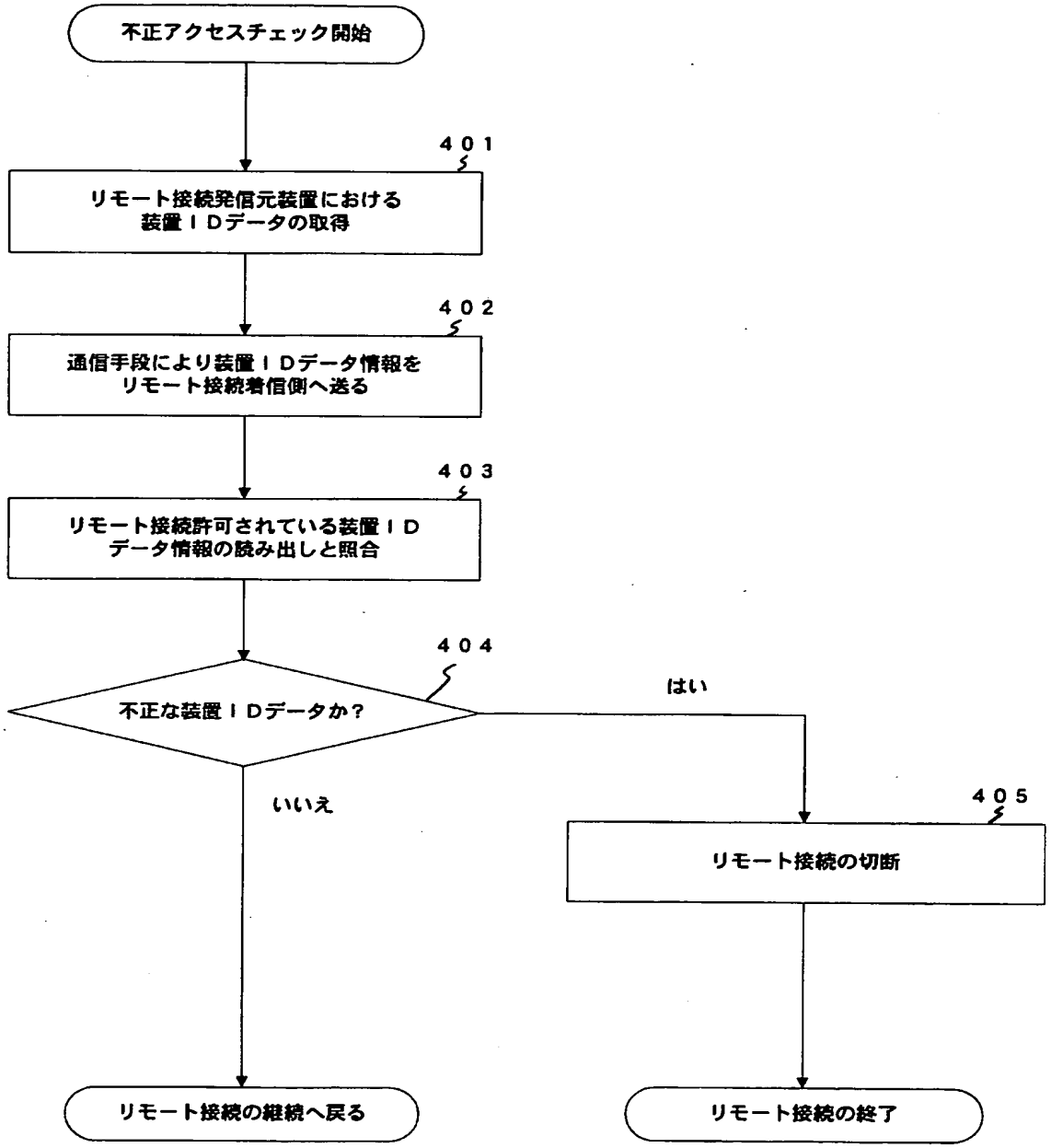
【図２】


不正アクセスチェック開始
２０１
リモート接続発信元装置における
ＧＰＳ受信データの取得
２０２
通信手段によりＧＰＳ受信データ情報を
リモート接続着信側へ送る
２０３
リモート接続許可されている装置設置場所と
ＧＰＳ受信データとの照合
２０４
不正な設置場所データあるいは
無効なＧＰＳデータか？
はい
いいえ
２０５
リモート接続の切断
リモート接続の継続へ戻る
リモート接続の終了

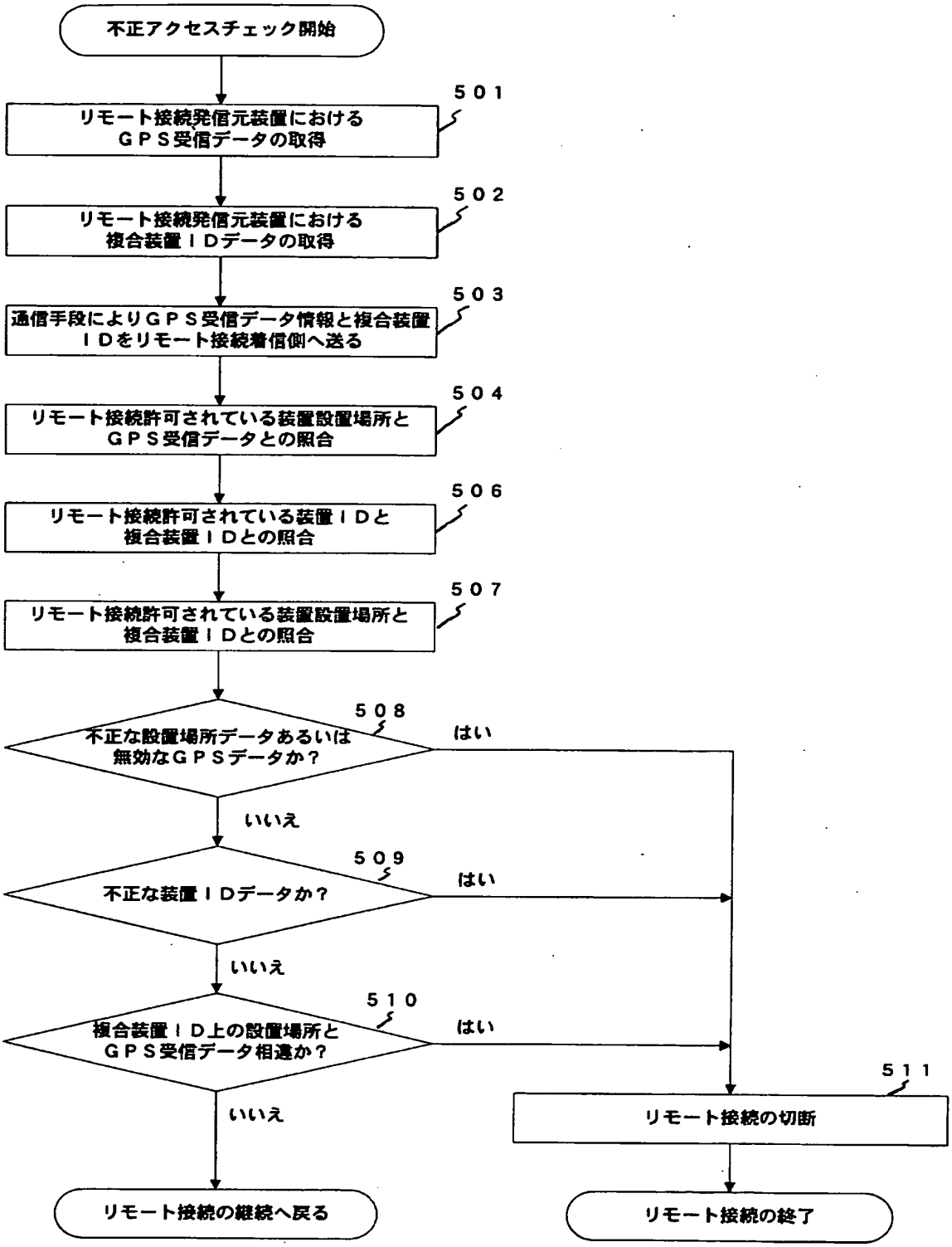
【図３】



【図４】


不正アクセスチェック開始
401
リモート接続発信元装置における
装置ＩＤデータの取得
402
通信手段により装置ＩＤデータ情報を
リモート接続着信側へ送る
403
リモート接続許可されている装置ＩＤ
データ情報の読み出しと照合
404
不正な装置ＩＤデータか？
はい
いいえ
405
リモート接続の切断
リモート接続の継続へ戻る
リモート接続の終了

【図５】


不正アクセスチェック開始
５０１
リモート接続発信元装置における
ＧＰＳ受信データの取得
５０２
リモート接続発信元装置における
複合装置ＩＤデータの取得
５０３
通信手段によりＧＰＳ受信データ情報と複合装置
ＩＤをリモート接続着信側へ送る
５０４
リモート接続許可されている装置設置場所と
ＧＰＳ受信データとの照合
５０６
リモート接続許可されている装置ＩＤと
複合装置ＩＤとの照合
５０７
リモート接続許可されている装置設置場所と
複合装置ＩＤとの照合
５０８
不正な設置場所データあるいは
無効なＧＰＳデータか？
はい
いいえ
５０９
不正な装置ＩＤデータか？
はい
いいえ
５１０
複合装置ＩＤ上の設置場所と
ＧＰＳ受信データ相違か？
はい
いいえ
５１１
リモート接続の切断
リモート接続の継続へ戻る
リモート接続の終了

【書類名】　　要約書

【要約】

【課題】　不正なリモートアクセスを確実に防止できるようにする。

【解決手段】　半導体露光装置とサーバ機１５０等との間でのリモートアクセスが開始されると、半導体露光装置では、ＧＰＳ受信機１０８により当該半導体露光装置が現在設置されている場所の緯度経度情報が取得されて、そのＧＰＳ受信データ（緯度経度情報）が通信インターフェース１０９及び通信装置１１６を介してサーバ機１５０等へ送出され、サーバ機１５０等では、受信したＧＰＳ受信データによる装置設置場所の緯度経度情報をリモートアクセスを許可すべきユーザ装置設置場所の緯度経度情報と比較・照合して、不正な設置場所データ、或いは改ざん、偽造による無効なＧＰＳ受信データであると判断した場合には、リモートアクセスを切断する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００１００７〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都大田区下丸子３丁目３０番２号
氏　名　キヤノン株式会社